TECHNICAL INSIGHTS

SENSOR

TECHNOLOGY ALERT

01st August 2014

1. ALL-OPTICAL ULTRA HIGH-TEMPERATURE FIBER OPTIC SENSOR

Fiber optic sensors can provide key benefits compared to conventional electronic sensors, such as immunity to electromagnetic interference, multiplexing capability, high sensitivity, high temperature range, as well as active power, and in certain configurations, the ability to sense at multiple points along the fiber. Such sensors are also capable of sending and receiving signals over long distances for increased application flexibility.

Researchers at the University of Pittsburgh have extended the capabilities of fiber optic sensors by leveraging the high temperature capability of such sensors and the ability of fiber optic sensors to provide optical power as well as signal transmission and sensing.

The researchers created an all-optical high-temperature sensor for gas flow measurements that operates at ultra-high temperatures above 800 degrees C by fusing together the concepts of active fiber sensors and high-temperature fiber sensors.

The researchers overcame the challenge of achieving active measurements in optical fiber. They enabled the same fiber to be used for both signal transmission and for energy delivery or optical power for active measurement. Such capability significantly improves the sensitivity, functionality, and agility of fiber optic sensors.

The team has demonstrated simultaneous flow/temperature sensors operating at 850 degrees C, an improvement of 200 degrees C on an earlier, key demonstration of microelectromechanical systems (MEMS)-based sensors by researchers at Oak Ridge National Laboratory.

The essential concept involves integrating optical heating elements, optical sensors, an energy delivery cable and a signal cable within a single optical fiber. Optical power delivered by the fiber is used to provide energy to the heating element; and the optical sensor within the same fiber measures the heat transfer from the heating element and transmits it back, creating a smart optical fiber sensor powered by in-fiber light.

Tapping into the energy carried by the optical fiber can allow for sensors that are able to perform more sophisticated and multifunctional measurements and to expand the use of fiber optic sensors beyond temperature and strain measurements.

In microgravity environments, for example, it can be challenging to measure the level of liquid hydrogen fuel in tanks, as the liquid hyrdrogen does not settle at the bottom of the tank. In such an application, optical fiber sensors are capable of reducing the wiring that is required when using numerous electronic sensors. Many sensors can be packed into a single optical fiber to reduce or eliminate the wiring issues associated with having numerous wires or leads to deliver a sensing signal.

The technology also lends itself to development of highly sensitive chemical sensors for cryogenic environments. The optical energy in the fiber can be tapped to locally heated in-fiber chemical sensors for enhanced sensitivity. The in-fiber optical power can also be converted into ultrasonic or microwave energy or into other applications, since numerous (for example, tens or hundreds) of smart sensors can be multiplexed within a single fiber. One fiber would be able to be placed in the gas flow stream, even in locations that have strong magnetic interference.

This technology can find industrial sensing applications in harsh environments, such as deep geothermal drill cores, the interiors of nuclear reactors, or space missions, and may over time be extended into other application areas.

The team plans to explore ways to enhance the optical cable for fiber sensing. They have planned to address issues such as scrutinizing the size or shape of the fiber to better suit particular applications, and the possibility of carrying other types of energy along the fibers for long distance and remote sensing.

Details: Kevin P. Chen, Associate Professor and the Paul E. Lego Faculty Fellow, Department of Electrical and Computer Engineering, University of Pittsburg, Pittsburgh, PA 15261. Phone: 412-624-9675; E-mail: pec9@pitt.edu

2. ADVANCEMENTS IN DETECTION OF EXPLOSIVES IN MOBILE DEVICES

Currently, there is increasing concern for being able to very accurately detect explosives concealed in mobile electronic devices. Opportunities for detection of explosives in mobile devices on airplanes have been enhanced by very recent security measures requiring travelers on flights originating from Europe, Africa, and the Middle East and going directly to the US and UK to power up their electronic devices for security screening. The new security measures could slow international security checkpoints and delay passengers or require that they surrender their electronic devices.

There have been key challenges in effective explosives detection, including the need for rapid detection without false alarms.

Nuclear quadrupole resonance (NQR) technology uses radio waves to excite quadrupole atoms in order to create a moment with the nuclear spins. The wavelength spectrum of the energy re-emitted by the stimulated atoms can then be utilized to identify the molecule of interest. RF pulses cause the nuclei of explosives to resonate and create an electric potential in the receiver coil. NQR is essentially based on magnetic resonance imaging (MRI) technology. In NQR, a radio frequency (RF) technique is used to detect target chemical compounds. In contrast to nuclear magnetic resonance (NMR), NQR does not rely on an external static magnetic field to align nuclei. Instead, NQR uses the internal electric field gradient of the material.

NQR is effective in detecting, for example, the nitrogen isotope N-14, which has been a component in many forms of high explosives as well as narcotics. NQR can have a very low false alarm rate due to, for example, other nitrogen-containing materials. Moreover, the NQR approach can have advantages in sensing explosives over other methods, such as bomb-sniffing dogs and vapor detectors, which can be influenced by environmental conditions (such as wind or ground moisture) and may not be able to adequately detect hermetically-sealed explosives.

Reflecting opportunities for enhanced detection of explosives in mobile devices, US-based One Resonance Sensors (ORS) has unveiled a portable electronics scanner, the MobiLab ES, which uses chemical-specific quadrupole resonance radio frequency sensing technology to detect explosives and precursors in mobile electronics devices such as mobile phones or chargers.

Such technology can enable airport security to rapidly inspect electronic devices.

The MoliLab ES portable electronics scanner, which leverages development from the MobiLab® BLS (bottled liquid screener) is compact with no moving parts, offers one-touch operation, and is self-calibrating.

Details: Dr. Pablo Prado, Co-Founder and CEO, One Resonance Sensors, LLC, 2878 Camino del Rio South, Suite 115, San Diego, CA 92108. Phone: 619-501-5750. E-mail: Pablo.prado@dteect-ors.com

3. ADVANCEMENTS IN PARTIAL DISCHARGE DETECTION

A partial discharge is a localized dielectric breakdown of a portion of the insulation when under high voltage stress. The localized dielectric breakdown does not bridge the space between the two conductors. Detection of partial discharges before they erode the insulation and, thereby, potentially result in a catastrophic failure is vital for ensuring the health of electric utility transformers.

The utility industry has used various techniques to detect partial discharges, such as measuring the impedance and induced apparent charge in a detection circuit via, for example, coupling capacitor sensors, current transformers, Rogowski coils; acoustic emission (sense acoustic emissions generated by a source of partial discharge); ultra high frequency (UHF) measurement of radio waves; or dissolved gas analysis (detection of hydrogen, methane or other gases in the transformer can indicate a partial discharge. Also, sparking discharges in oil or paper can create significant hydrocarbons such as acetylene.

Conventional techniques for detecting partial discharge in utility transformers can have limitations, such as susceptibility to noise or to false alarms, inability to detect the exact location of the partial discharge, low sensitivity, inconvenience for use in continuous monitoring, complex signal processing, and so on.

There is a vital need for a sensing solution that is able to provide continuous, real-time monitoring of partial discharge (or of other potential faults) in utility transformers and provide an early warning of a potential failure or catastrophic event. Such needs are especially prevalent for high-value transformers such as large power transformers.

Micro-electromechanical systems (MEMS) sensors that can be easily and conveniently placed inside the transformer to provide more precise, early detection of the location and magnitude of a partial discharge offer promise for improved condition monitoring of an incipient partial discharge in utility transformers . The use of sophisticated data processing and wireless communications, moreover, can provide personnel with vital, real-time information that can help to lessen or possibly eliminate damage to a transformer due to partial discharge.

Details: Peter Adrian, Principal Analyst, Technical Insights, Frost & Sullivan, 331 E. Evelyn Avenue, Suite 100, Mountain View, CA 94041. Phone: 408-972-1865/650-475-4523. E-mail: peter.adrian@frost.com. URL: www.frost.com

4. RECENT PATENTS IN THE FIELD OF BIOMETRIC SENSING

The increase in terrorist attacks and crime rates across the world has necessitated reliable authentication systems. Biometric authentication is a key method to identify a person. In biometrics, physiologic or behavioral features, such as the palm, fingerprint, face, iris, voice, or vein, are used to verify the identity of the user.

To collect the digital image of the fingerprint, key types of fingerprint sensor technologies include optical, capacitive, ultrasonic, thermal, and radio frequency and pressure sensors. For palm recognition, sensor technologies such as capacitive, optical, ultrasound, and thermal can be used to collect a digital image of the palm's surface. Biometric authentication processes compare the biometrics of the user with the data stored in the database and then determine whether the person is legitimate or not. The use of multi-mode biometrics, such as combining fingerprint capture, iris scan, and face capture or face recognition, has opportunities to assure higher accuracy of the biometric identification system.

A recent patent in biometric sensing (WO/2014/112081), assigned to Fujitsu Limited, involves the incorporation of three units, that is, reading sensor, client, and server. The reading sensor unit comprises a fingerprint sensor unit and vein sensor unit. The server includes a memory unit, storage unit, communication unit, server control unit, fingerprint comparison unit and vein comparison unit. The client unit consists of a client control unit, finger print comparison unit, vein control unit, memory unit, communication unit, left/right hand input check unit, left/right correspondence table, and rotation prediction unit. The three units are connected to each other with a binary unit system (BUS). The Bus is a transmission path where signals are picked up and dropped at every device attached to the Bus line.

The biometric authentication device works on the principle of comparison; and works for both the left and right hand. If a client scans his/her left hand on the reading senor unit, it passes on the information to the client unit. The client unit detects the scanned hand by the left/right input check unit and passes on the data to the fingerprint comparison unit. The fingerprint comparison unit sends the data to the storage unit in the server section through a Bus. If the client already exists in the database, the server section will authenticate the client and provides authentication results. If the client does not exist or his information is not stored in the database, the server section will store the information of the client in the storage unit for future use. In this way, the biometric authentication device can provide authentic results.

PATENT TITLE	PUBLICATION DATE / NUMBER	ASSIGNEE	INVENTORS	ABSTRACT
Biometric Authentication Device, Biometric Authentication System, And Biometric Authentication Method	24.07.2014; WO/2014/112081	FUJITSU LIMITED	AOKI, Takahiro	A biometric authentication device having: a single reading sensor that acquires first comparison-use authentication characteristic data, which is specific to one hand and is used for comparison, and second comparison-use authentication characteristic data, which is specific to the other hand and is used for comparison; and a communication unit that transmits both the first comparison-use authentication characteristic data and the second comparison-use authentication characteristic data for one person to the outside as authentication data, and receives an authentication result.
METHOD AND SYSTEM FOR PROVIDING PRODUCT IDENTIFICATION INFORMATION	24.07.2014; WO/2014/112874	MOBA GROUP B.V.	DE VLAAM, Hendrikus Louis Stephanus	Method for providing products identification information, comprising: -providing a number of food products (P) of at least one product type, the products of each product type differing mutually in at least one characteristic; -detecting the at least one characteristic of each of the products; -on the basis of the detected characteristic of each of the products, generating an identification information unique to each product; and -storing the identification information of the products in a memory (10). The invention further

				concerns a system for providing products identification information for carrying out the above method. With great advantage, the origin of the products can therewith be checked and thus guaranteed. Furthermore, modern technologies, including GPS applications and smart phones, can be deployed in a handy manner and accessible to everyone.
BIOMETRIC IMAGING DEVICES AND ASSOCIATED METHODS	24.07.2014; WO/2014/113728	SIONYX, INC..	SAYLOR, Stephen D	Systems, devices, and methods for authenticating an individual or user using biometric features is provided. In one aspect, for example, a system for authenticating a user through identification of at least one biometric feature can include an active light source capable of emitting electromagnetic radiation having a peak emission wavelength at from about 700 nm to about 1200 nm, where the active light source is positioned to emit the electromagnetic radiation to impinge on at least one biometric feature of the user, and an image sensor having infrared light-trapping pixels positioned relative to the active light source to receive and detect the electromagnetic radiation upon reflection from the at least one biometric feature of the user. The system can further include a processing module functionally coupled to the image sensor and operable to generate an electronic representation of the at least one biometric feature of the user from detected electromagnetic radiation, and an authentication module functionally coupled to the processing module that is operable to receive and compare the electronic representation to an authenticated standard of the at least one biometric feature of the user to provide authentication of the user.
DETECTION SYSTEM FOR DETECTING PRESENCES OR TIMES	24.07.2014; WO/2014/111763	STUDIO ZIVERI S.R.L.	ZIVERI, Eleonora	A detection system (1) for detecting presences or times, comprising: a telecommunications network (2); at least one monitor (3) configured to project images; at least one generating module (4) for generating varying codes, and connected to the monitor (3); one or more mobile devices (10), each of which having onboard an optical sensor (5) configured to detect the codes projected by the monitor (3) and at least one transmission module (6) that transmits these codes to the telecommunications network (2); a receiving module (7) connected to the telecommunications

				network (2) and configured to receive the codes from the mobile device (10).
SECURE REAL-TIME HEALTH RECORD EXCHANGE	24.07.2014; WO/2014/113817	HUMETRIX. COM, INC.	EXPERTON, Bettina	A method, an apparatus, and a computer program product for accessing electronic medical records are provided in which a portable computing device uniquely associated with a user authenticates an identification of the user and automatically retrieves information corresponding to the user from electronic healthcare records systems using the identification. The retrieved information may be combined with other information and electronically delivered to a healthcare provider or patient. Delivery may be initiated by the portable computing device and directed to a computing device of a healthcare provider or patient. Exchange of records and other information between the user and the provider is effected using a first channel to provide a network address of the records and cryptographic keys necessary to extract the records, and a second path to deliver the encrypted records. The first path may be implemented using a camera or optical scanner to read an encoded optical image.
SYSTEMS AND METHODS FOR DISTRIBUTED ENHANCED PAYMENT PROCESSING	24.07.2014; WO/2014/113596	MERCURY PAYMENT SYSTEMS, LLC	OZVAT, Matthew, D.	A distributed enhanced payment processing system includes a merchant point of sale (POS) terminal system and a remote payment management system. The POS terminal system initiates a transaction that includes receiving a payment amount, a purchaser account identifier, a virtual electronic payment indicator, and a merchant ID via a payment client. Subsequently, the POS terminal system outputs the transaction to the remote payment management system which generates a token for the transaction. The payment management system then provides the purchaser account identifier, a merchant account identifier, and the payment amount to a remote virtual electronic payment (VEP) entity system. Upon receiving a VEP entity system response, the payment management system outputs the response and token to the POS terminal system.

MOUNTING BRACKET AND PROTECTIVE ENCLOSURE	24.07.2014; WO/2014/111757	TROJAN DEVELOPMENTS LTD.	JACKSON, Nigel, Glenn	One embodiment relates to a protective enclosure for use with an access control system. The protective enclosure comprises a base plate for mounting an emergency door opener to a support, and a cover plate coupled to the base plate for movement between a closed position in which the emergency door opener is enclosed, and an open position in which the emergency door opener is accessible for emergency operation. Another embodiment relates to a circuit board mounting bracket comprising a base member with spaced apart sidewalls that define an interior cavity, and a plurality of fingers extending upwardly from the sidewalls for gripping a circuit board located within the interior cavity. The fingers are separated by gaps for receiving wires that are connected to the circuit board. The mounting bracket also includes a cover mountable to the base member, which may protect the wires and allow labeling of the circuit board.

Exhibit 1 lists some of the patents related to biometric sensing.

Picture Credit : Frost & Sullivan

Back to TOC